Claims

[c1] 1. A data protection device by using address, performing a data protection operation by controlling an access of a data in a Basic Input/Output System (BIOS), the device comprising:
a memory device, wherein the memory device builds a database according to the address of the data in the BIOS, and the database records a usage authorization of the data and a password for releasing the usage authorization; and
an address decoder, wherein the address decoder couples to a chipset, the BIOS, and the memory device, the address decoder receives and decodes a control signal to obtain an usage information, compares with the address and the usage authorization, and receives an authentication password;
wherein the address decoder restricts the control that the chipset applies to the data according to the usage authorization, and receives the authentication password that is sent to the address decoder, compares the password, and releases the usage authorization.

[c2] 2. The data protection device by using address of claim 1, wherein the memory device and the address decoder can be integrated into the chipset.

[c3] 3. The data protection device by using address of claim 1, wherein the memory device, the address decoder and the BIOS can be integrated into a chipset.

[c4] 4. The data protection device by using address of claim 1, wherein the memory device can build a database according to an address range that includes a plurality of data records in the BIOS, and the database records a usage authorization of the plurality of data records and a password to release the usage authorization of the plurality of data records.

[c5] 5. The data protection device by using address of claim 1, wherein the authentication password can be provided by a keyboard, a mouse, an encryption/decryption engine, a smart card, a key or a biotic characteristic.

[c6] 6. The data protection device by using address of claim 1, wherein the address decoder further sends out a warning signal when the chipset exceeds the data

usage authorization or when the authentication password is not accepted.

[c7] 7. The data protection device by using address of claim 5, wherein the biotic characteristic comprises either a fingerprint or a sound waveform.

[c8] 8. The data protection device by using address of claim 5, wherein the authentication password can be provided by a combination of the keyboard, the mouse, the encryption/decryption engine, the smart card, the key and the biotic characteristic.

[c9] 9. A data protection device by using address, performing a data protection operation by controlling an access of a data in a hard disk, the device comprising:
a memory device, wherein the memory device builds a database according to the address of the data in the hard disk, and the database records a usage authorization of the data and a password for releasing the usage authorization; and
an address decoder, wherein the address decoder couples to a chipset, the hard disk, and the memory device, the address decoder receives and decodes a control signal to obtain a usage information, compares with the address and the usage authorization, and receives an authentication password;
wherein the address decoder restricts the control that the chipset applies to the data according to the usage authorization, and receives the authentication password that is sent to the address decoder, compares the password, and releases the usage authorization.

[c10] 10. The hard disk data protection device by using address of claim 9, wherein the memory device and the address decoder can be built-in inside the chipset.

[c11] 11. The hard disk data protection device by using address of claim 9, wherein the memory device and the address decoder can be built-in inside the hard disk.

[c12] 12. The hard disk data protection device by using address of claim 9, wherein the memory device and the address decoder can be built-in inside an integrated circuit (IC) that controls a redundant array of intelligent disks (RAID).

[c13] 13. The hard disk data protection device by using address of claim 9, wherein the memory device can build a database according to an address range that includes a plurality of data records in the hard disk, and the database records a usage authorization of the plurality of data records and a password to release the usage authorization of the plurality of data records.

[c14] 14. The hard disk data protection device by using address of claim 9, wherein the authentication password can be provided by a keyboard, a mouse, an encryption/decryption engine, a smart card, a key or a biotic characteristic.

[c15] 15. The hard disk data protection device by using address of claim 9, wherein the address decoder further sends out a warning signal when the chipset exceeds the data usage authorization or when the authentication password is not accepted.

[c16] 16. The hard disk data protection device by using address of claim 14, wherein the biotic characteristic comprises either a fingerprint or a sound waveform.

[c17] 17. The hard disk data protection device by using address of claim 14, wherein the authentication password can be provided by a combination of the keyboard, the mouse, the encryption/decryption engine, the smart card, the key and the biotic characteristic.